FIG. 1

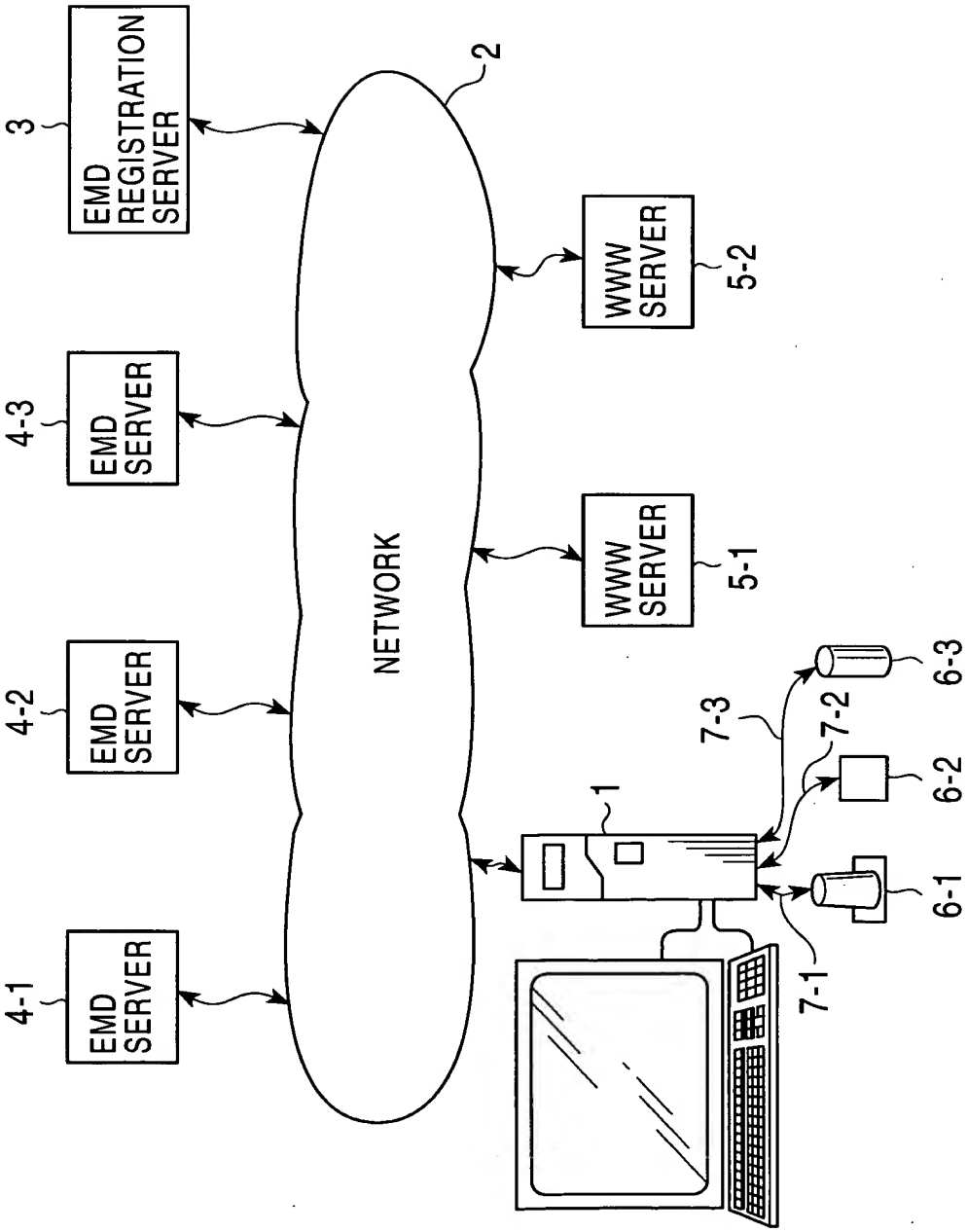

3
EMD REGISTRATION SERVER
2
NETWORK
4-3
EMD SERVER
4-2
EMD SERVER
4-1
EMD SERVER
WWW SERVER
5-2
WWW SERVER
5-1
1
7-3
7-2
7-1
6-3
6-2
6-1

FIG. 2

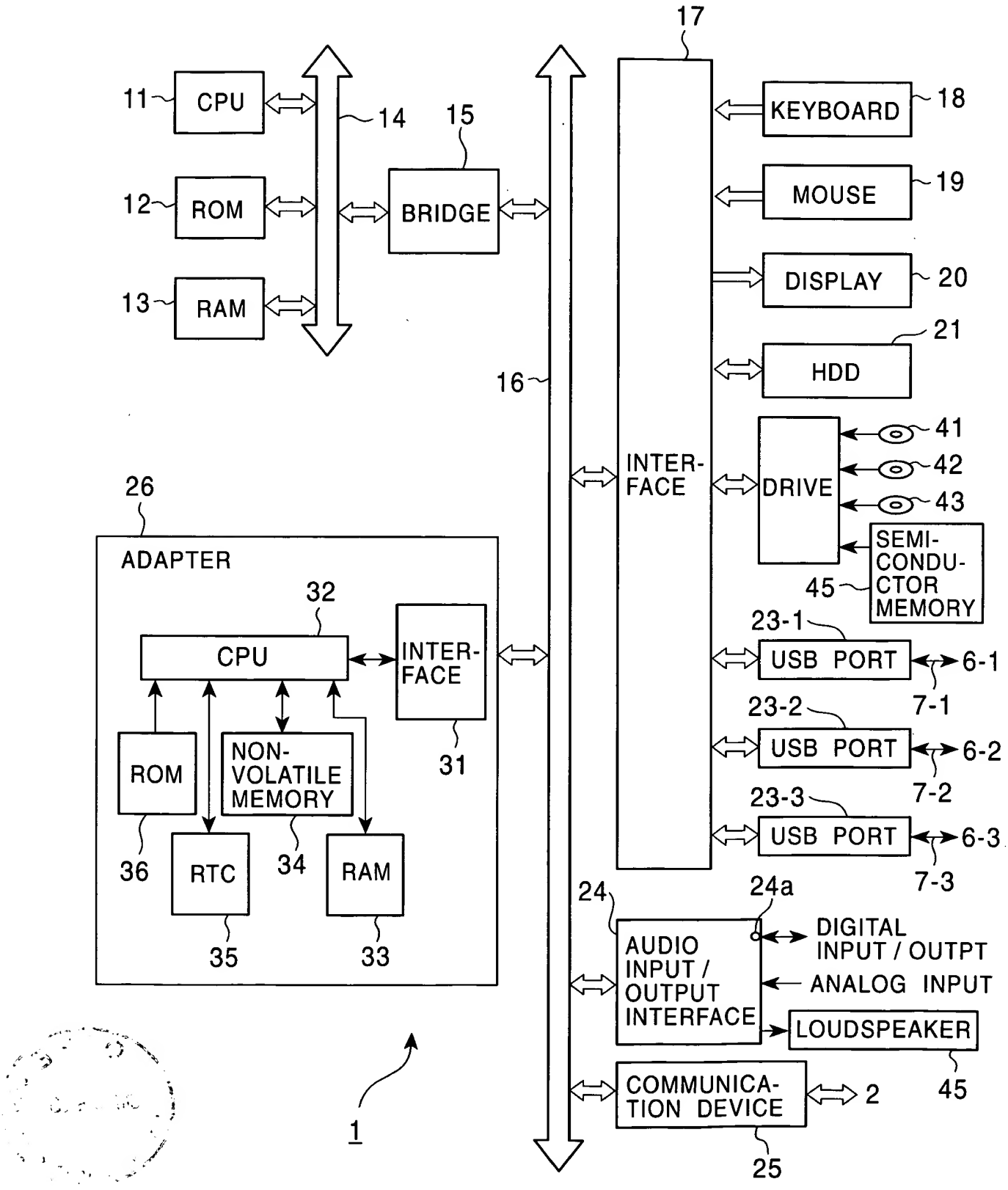

17
11
CPU
14
15
12
ROM
BRIDGE
13
RAM
16
KEYBOARD
18
MOUSE
19
DISPLAY
20
21
HDD
INTER-
FACE
DRIVE
41
42
43
SEMI-
CONDU-
CTOR
MEMORY
45
26
ADAPTER
32
CPU
INTER-
FACE
31
ROM
NON-
VOLATILE
MEMORY
36
RTC
34
RAM
35
33
23-1
USB PORT
6-1
7-1
23-2
USB PORT
6-2
7-2
23-3
USB PORT
6-3
7-3
24
24a
AUDIO
INPUT /
OUTPUT
INTERFACE
DIGITAL
INPUT / OUTPT
ANALOG INPUT
LOUDSPEAKER
45
COMMUNICA-
TION DEVICE
2
25
1

FIG. 3

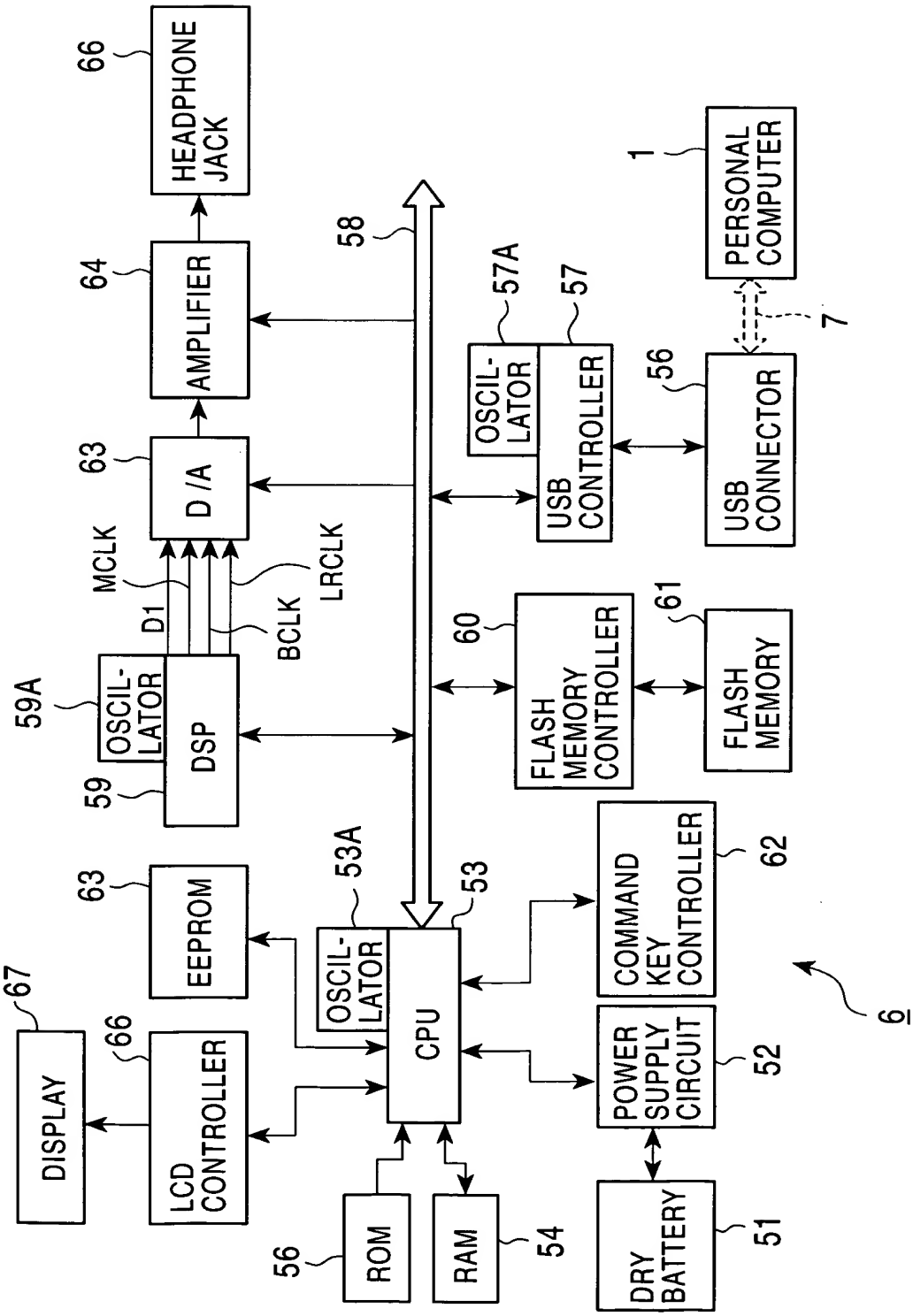

HEADPHONE JACK
66
AMPLIFIER
64
D /A
63
MCLK
D1
BCLK
LRCLK
OSCIL-LATOR
59A
DSP
59
58
OSCIL-LATOR
57A
USB CONTROLLER
57
USB CONNECTOR
56
PERSONAL COMPUTER
1
7
FLASH MEMORY CONTROLLER
60
FLASH MEMORY
61
EEPROM
63
OSCIL-LATOR
53A
CPU
53
COMMAND KEY CONTROLLER
62
DISPLAY
67
LCD CONTROLLER
66
POWER SUPPLY CIRCUIT
52
ROM
56
RAM
54
DRY BATTERY
51
6

FIG. 4

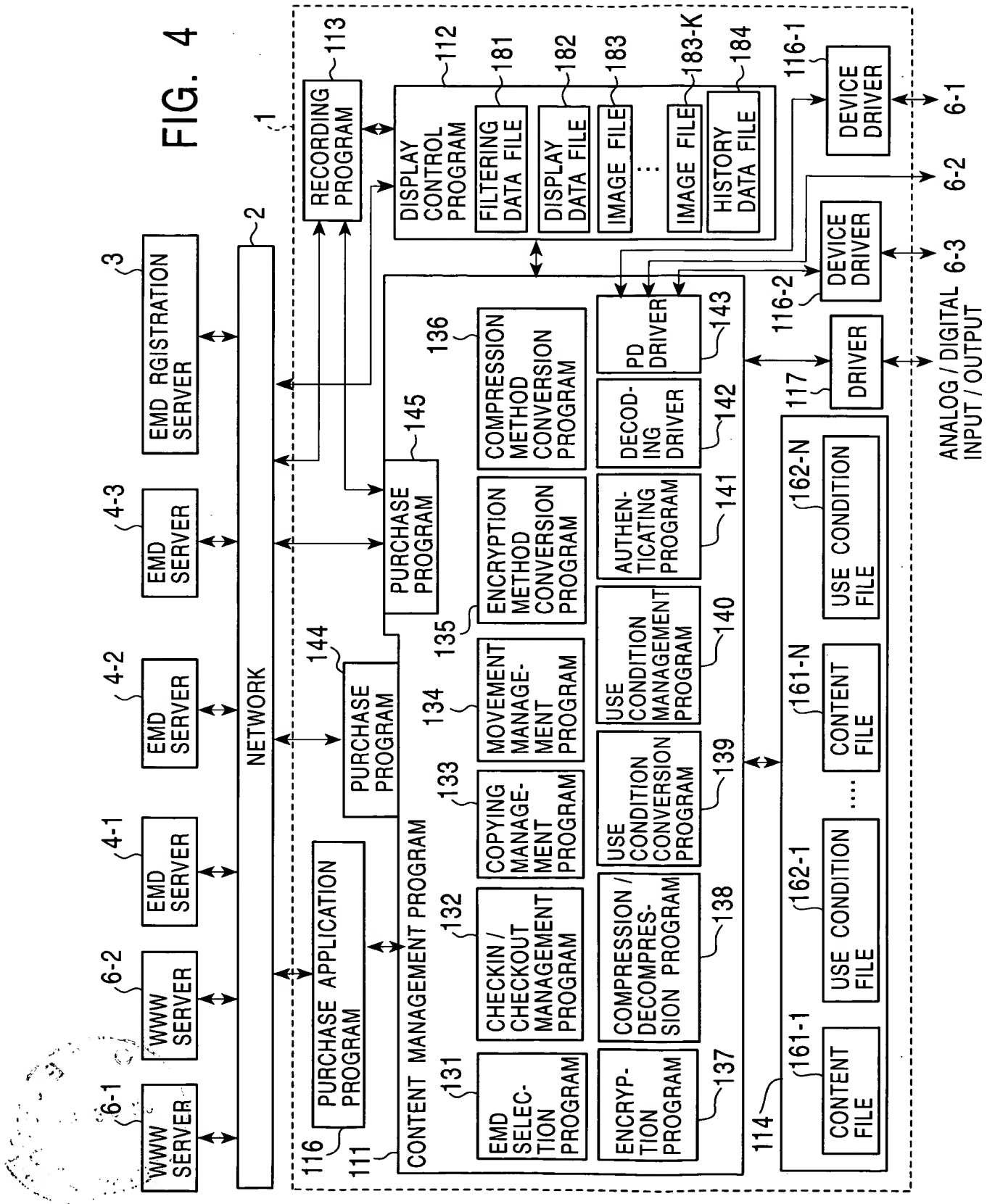

WWW SERVER
6-1
WWW SERVER
6-2
EMD SERVER
4-1
EMD SERVER
4-2
EMD SERVER
4-3
EMD RGISTRATION SERVER
3
NETWORK
2
1
RECORDING PROGRAM
113
DISPLAY CONTROL PROGRAM
112
FILTERING DATA FILE
181
DISPLAY DATA FILE
182
IMAGE FILE
183
IMAGE FILE
183-K
HISTORY DATA FILE
184
DEVICE DRIVER
116-1
DEVICE DRIVER
116-2
DRIVER
117
PD DRIVER
143
DECOD-ING DRIVER
142
AUTHEN-TICATING PROGRAM
141
USE CONDITION MANAGEMENT PROGRAM
140
USE CONDITION CONVERSION PROGRAM
139
COMPRESSION METHOD CONVERSION PROGRAM
136
ENCRYPTION METHOD CONVERSION PROGRAM
135
MOVEMENT MANAGE-MENT PROGRAM
134
COPYING MANAGE-MENT PROGRAM
133
CHECKIN / CHECKOUT MANAGEMENT PROGRAM
132
COMPRESSION / DECOMPRES-SION PROGRAM
138
ENCRYP-TION PROGRAM
137
EMD SELEC-TION PROGRAM
131
PURCHASE PROGRAM
145
PURCHASE PROGRAM
144
PURCHASE APPLICATION PROGRAM
116
CONTENT MANAGEMENT PROGRAM
111
USE CONDITION FILE
162-N
CONTENT FILE
161-N
USE CONDITION FILE
162-1
CONTENT FILE
161-1
114
ANALOG / DIGITAL INPUT / OUTPUT
6-3
6-2
6-1

FIG. 5

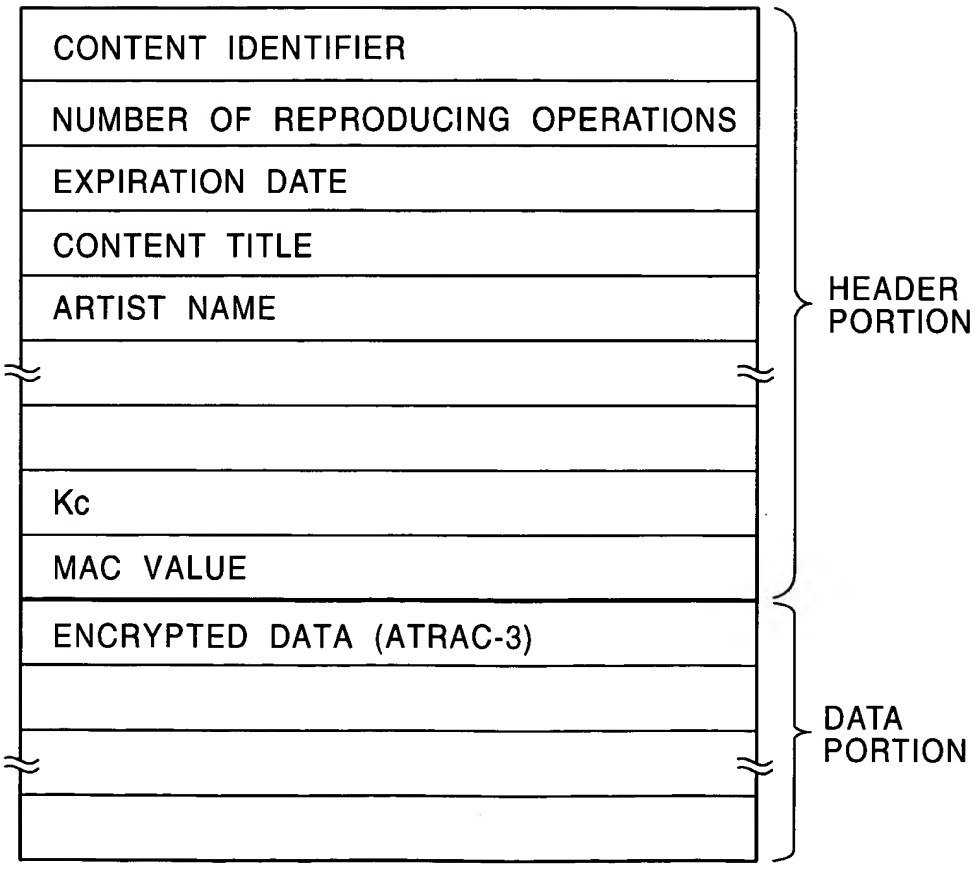

CONTENT IDENTIFIER
NUMBER OF REPRODUCING OPERATIONS
EXPIRATION DATE
CONTENT TITLE
ARTIST NAME
Kc
MAC VALUE
ENCRYPTED DATA (ATRAC-3)
HEADER PORTION
DATA PORTION

FIG. 6

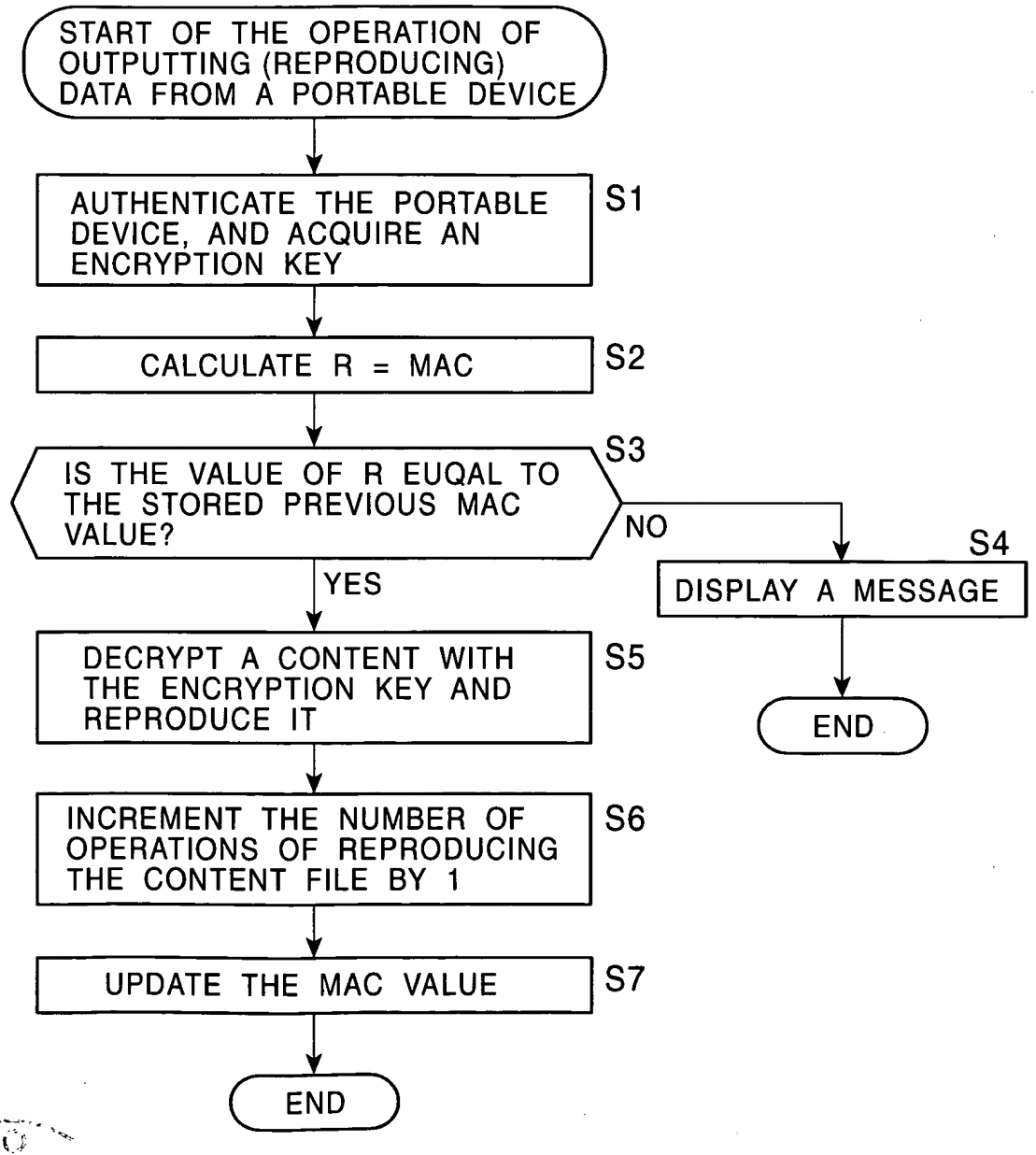

START OF THE OPERATION OF OUTPUTTING (REPRODUCING) DATA FROM A PORTABLE DEVICE
AUTHENTICATE THE PORTABLE DEVICE, AND ACQUIRE AN ENCRYPTION KEY
S1
CALCULATE R = MAC
S2
IS THE VALUE OF R EUQAL TO THE STORED PREVIOUS MAC VALUE?
S3
NO
YES
DISPLAY A MESSAGE
S4
END
DECRYPT A CONTENT WITH THE ENCRYPTION KEY AND REPRODUCE IT
S5
INCREMENT THE NUMBER OF OPERATIONS OF REPRODUCING THE CONTENT FILE BY 1
S6
UPDATE THE MAC VALUE
S7
END

FIG. 7

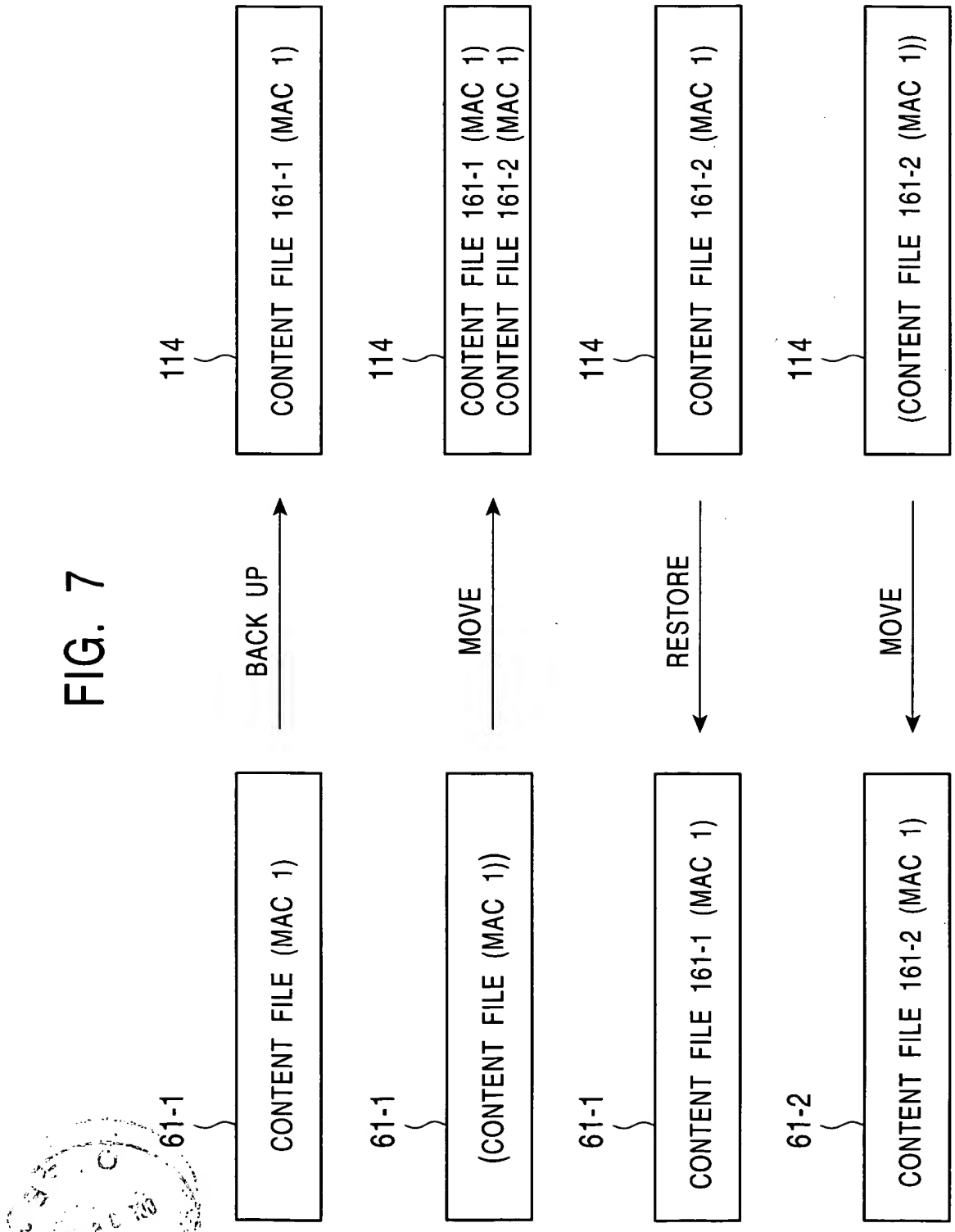

61-1
CONTENT FILE (MAC 1)
BACK UP
114
CONTENT FILE 161-1 (MAC 1)
61-1
(CONTENT FILE (MAC 1))
MOVE
114
CONTENT FILE 161-1 (MAC 1)
CONTENT FILE 161-2 (MAC 1)
61-1
CONTENT FILE 161-1 (MAC 1)
RESTORE
114
CONTENT FILE 161-2 (MAC 1)
61-2
CONTENT FILE 161-2 (MAC 1)
MOVE
114
(CONTENT FILE 161-2 (MAC 1))

FIG. 8A

	DEFECT (BAD) BLOCK	ALTERNATIVE BLOCK
0		
1		
2		
3		
4		
5		

FIG. 8B

seq 1
seq 2
seq 3
seq 4

FIG. 9

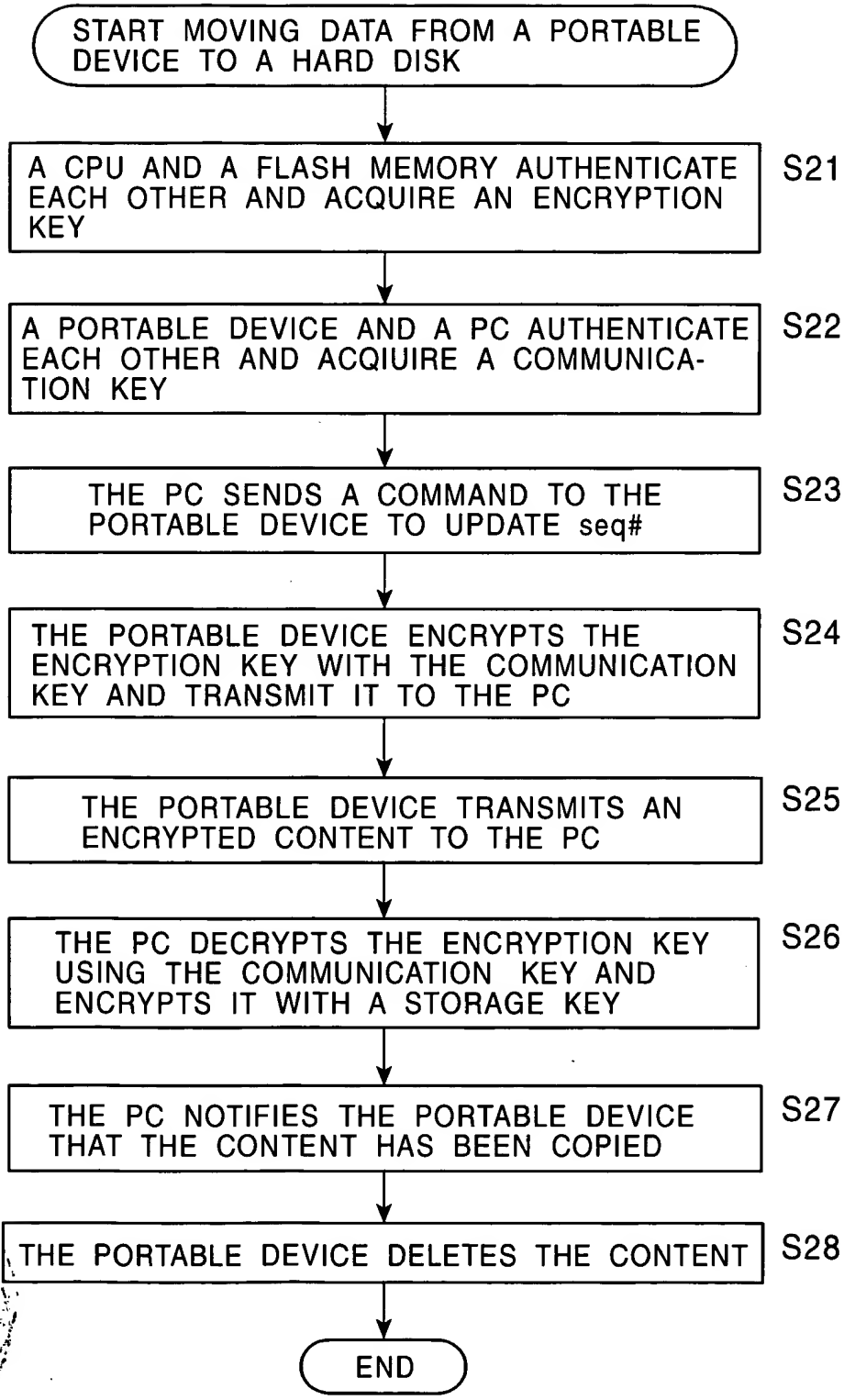
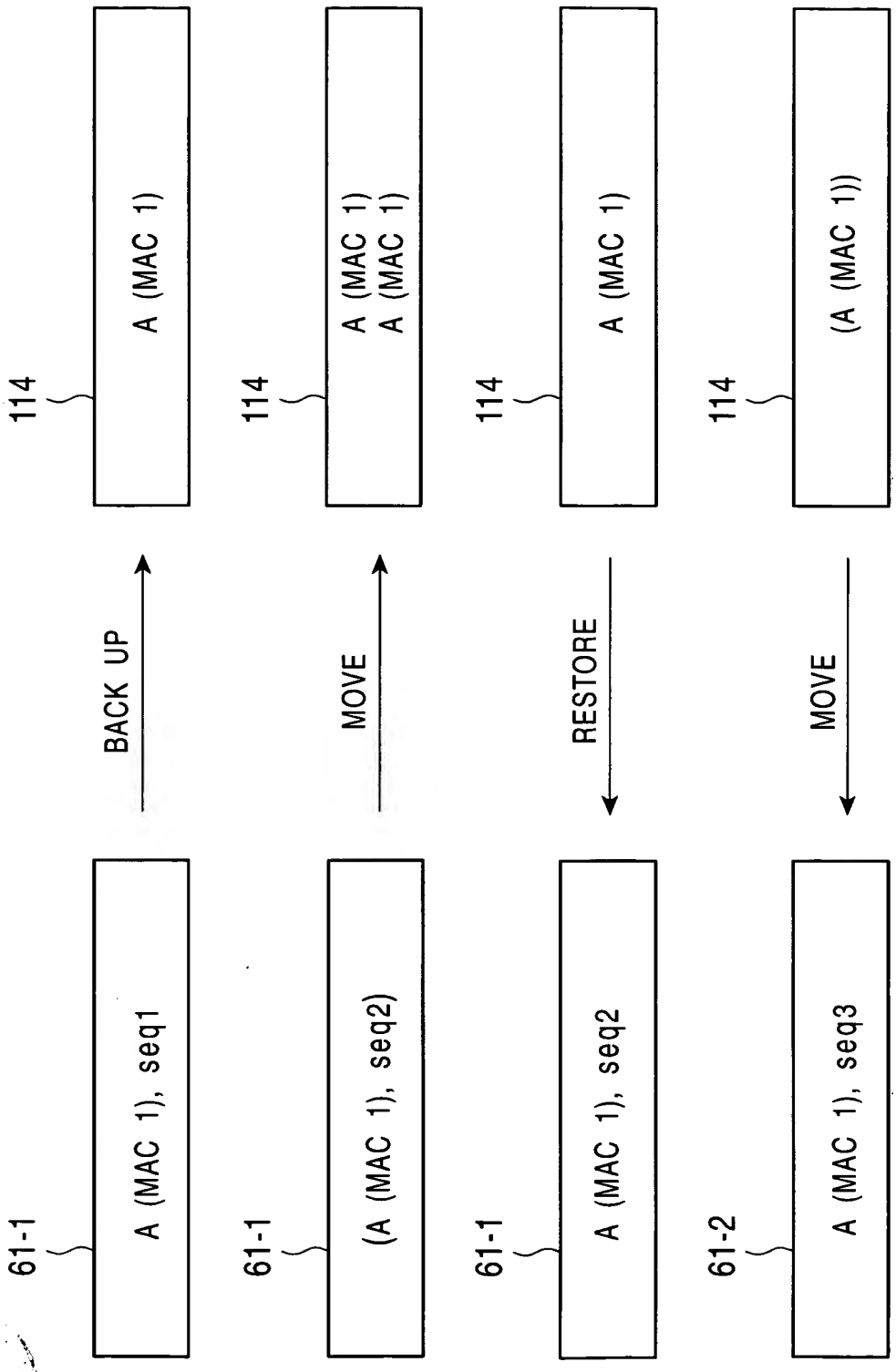

START MOVING DATA FROM A PORTABLE DEVICE TO A HARD DISK
A CPU AND A FLASH MEMORY AUTHENTICATE EACH OTHER AND ACQUIRE AN ENCRYPTION KEY
S21
A PORTABLE DEVICE AND A PC AUTHENTICATE EACH OTHER AND ACQIUIRE A COMMUNICATION KEY
S22
THE PC SENDS A COMMAND TO THE PORTABLE DEVICE TO UPDATE seq#
S23
THE PORTABLE DEVICE ENCRYPTS THE ENCRYPTION KEY WITH THE COMMUNICATION KEY AND TRANSMIT IT TO THE PC
S24
THE PORTABLE DEVICE TRANSMITS AN ENCRYPTED CONTENT TO THE PC
S25
THE PC DECRYPTS THE ENCRYPTION KEY USING THE COMMUNICATION KEY AND ENCRYPTS IT WITH A STORAGE KEY
S26
THE PC NOTIFIES THE PORTABLE DEVICE THAT THE CONTENT HAS BEEN COPIED
S27
THE PORTABLE DEVICE DELETES THE CONTENT
S28
END

FIG. 10


61-1
A (MAC 1), seq1
BACK UP
114
A (MAC 1)
61-1
(A (MAC 1), seq2)
MOVE
114
A (MAC 1)
A (MAC 1)
61-1
A (MAC 1), seq2
RESTORE
114
A (MAC 1)
61-2
A (MAC 1), seq3
MOVE
114
(A (MAC 1))